Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
MACIEJA SZPUNARJA,
predstavljeni 27. oktobra 2022[1]

Zadeva C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
proti
Premier ministre,
Ministère de la Culture

(Predlog za sprejetje predhodne odločbe, ki ga je vložil Conseil d'État (državni svet, Francija))

„Predhodno odločanje – Obdelava osebnih podatkov in varstvo zasebnega življenja na področju elektronskih komunikacij – Direktiva 2002/58/ES – Člen 15(1) – Možnost držav članic, da omejijo obseg nekaterih pravic in obveznosti – Obveznost predhodnega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločbe so zavezujoče – Podatki o civilni identiteti, ki ustrezajo IP-naslovu“

I. Uvod

1. Vprašanje hrambe nekaterih podatkov spletnih uporabnikov in dostopa do njih je vedno aktualno vprašanje, v zvezi s katerim se je v zadnjem času izoblikovala že zelo obsežna sodna praksa Sodišča.

2. S to zadevo se Sodišču ponuja priložnost, da znova obravnava to vprašanje v prenovljenem okviru boja proti kršitvam pravic intelektualne lastnine, storjenim izključno na spletu.

[1] Jezik izvirnika: francoščina.

II. Pravni okvir

A. Pravo Unije

3. V uvodnih izjavah 2, 6, 7, 11, 22, 26 in 30 Direktive 2002/58/ES[2] je navedeno:

„(2) Ta direktiva uveljavlja spoštovanje temeljnih pravic in upošteva načela, priznana zlasti z Listino o temeljnih pravicah Evropske unije [(v nadaljevanju: Listina)]. Zlasti pa želi ta direktiva zagotoviti popolno spoštovanje pravic, določenih v členih 7 in 8 navedene listine.

[…]

(6) Internet spreminja tradicionalne tržne strukture, ker ponuja skupno, globalno infrastrukturo za dobavo široke izbire elektronskih komunikacijskih storitev. Javno dostopne elektronske komunikacijske storitve prek interneta odpirajo nove možnosti uporabnikom, pa tudi nova tveganja za njihove osebne podatke in zasebnost.

(7) V primeru javnih komunikacijskih omrežij je treba sprejeti posebne zakone in druge predpise, s katerimi se zavarujejo temeljne pravice in svoboščine fizičnih oseb ter zakoniti interesi pravnih oseb, zlasti v zvezi s čedalje večjo zmogljivostjo samodejnega shranjevanja in obdelave podatkov, ki se nanašajo na naročnike in uporabnike.

[…]

(11) Ta direktiva, tako kot Direktiva [95/46/ES[3]], ne obravnava vprašanj varstva temeljnih pravic in svoboščin, povezanih z dejavnostmi, ki jih ne ureja pravni red Skupnosti. Zato ne spreminja obstoječega ravnotežja med posameznikovo pravico do zasebnosti in možnostjo držav članic, da sprejmejo ukrepe iz člena 15(1) te direktive, potrebne za zaščito javne varnosti, obrambe, državne varnosti (vključno z gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve državne varnosti) in izvajanje kazenske zakonodaje. Ta direktiva torej ne vpliva na zmožnost držav članic, da zakonito prestrezajo elektronska sporočila ali da sprejmejo druge ukrepe, če so potrebni iz katerega koli od teh namenov ter v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin[, podpisano v Rimu 4. novembra 1950], kakor jo razlaga Evropsko sodišče za človekove pravice v svojih sodbah. Taki ukrepi morajo biti ustrezni, dosledno sorazmerni z namenom in potrebni v demokratični družbi ter predmet primernih zaščitnih ukrepov v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin.

[…]

[2] Direktiva Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514).

[3] Direktiva Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355).

(22) Prepoved shranjevanja sporočil in s tem povezanih podatkov o prometu osebam, ki niso uporabniki ali ki nimajo privolitve uporabnikov, ni namenjena prepovedi vsakega samodejnega, vmesnega in prehodnega shranjevanja teh podatkov, dokler se to dogaja samo zaradi izvedbe prenosa v omrežju elektronskih komunikacij in pod pogojem, da podatki niso shranjeni dlje, kot je to potrebno za prenos in upravljanje prometa in da zaupnost podatkov ostane zagotovljena v času njihovega hranjenja. […]

[…]

(26) Podatki o naročnikih, ki se obdelajo v elektronskih komunikacijskih omrežjih zaradi vzpostavitve povezav in prenosa podatkov, vsebujejo podatke o zasebnem življenju fizičnih oseb in zadevajo pravico do spoštovanja njihove korespondence ali legitimne interese pravnih oseb. Takšni podatki se lahko shranijo le v obsegu, potrebnem za izvedbo storitve, za namen zaračunavanja in plačila medsebojnih povezav ter za določen čas. Vsaka nadaljnja obdelava takih podatkov […] je dovoljena samo takrat, kadar naročnik v to privoli na podlagi točnih in popolnih podatkov, ki jih dobi od ponudnika javno razpoložljivih elektronskih komunikacijskih storitev o vrsti nadaljnje obdelave, ki jo ta namerava izvajati, in o naročnikovi pravici, da ne da privolitve za tako obdelavo ali da jo umakne. […]

[…]

(30) Sistemi za zagotavljanje elektronskih komunikacijskih omrežij in storitev morajo biti zasnovani tako, da omejijo količino potrebnih osebnih podatkov na strogi minimum. […]“

4. Člen 2 te direktive, naslovljen „Opredelitve“, določa:

„[…]

Uporabijo se tudi naslednje opredelitve pojmov:

(a) ‚uporabnik‘ pomeni vsako fizično osebo, ki uporablja javno razpoložljivo elektronsko komunikacijsko storitev v zasebne ali poslovne namene, pri čemer ni nujno naročena na to storitev;

(b) ‚podatki o prometu‘ pomenijo katere koli podatke, obdelane za namen prenosa sporočila po elektronskem komunikacijskem omrežju ali zaradi zaračunavanja tega sporočila;

(c) ‚podatki o lokaciji‘ pomenijo vsakršne podatke, obdelane v elektronskem komunikacijskem omrežju ali v okviru elektronske komunikacijske storitve, ki razkrivajo zemljepisni položaj terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve;

(d) ‚sporočilo‘ (komunikacija) pomeni vsak podatek, ki se izmenjuje ali prenaša med končnim številom strank s pomočjo javno razpoložljive elektronske komunikacijske storitve. To ne vključuje nobenih podatkov, prenesenih javnosti kot del radiodifuzijske storitve prek elektronskega komunikacijskega omrežja, razen v obsegu, v katerem se da podatek povezati s prepoznavnim naročnikom ali uporabnikom, ki ga prejme;

[…]“

5. Člen 3 navedene direktive, naslovljen „Storitve“, določa:

„Ta direktiva se uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Skupnosti, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave.“

6. Člen 5 te direktive, naslovljen „Zaupnost sporočil“, določa:

„1. Države članice s svojo nacionalno zakonodajo zagotovijo zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev. Zlasti prepovejo vsem osebam razen uporabnikom, da poslušajo, prisluškujejo, shranjujejo ali na druge načine prestrezajo ali nadzirajo komunikacije (sporočila) in z njimi povezane podatke o prometu, brez privolitve zadevnih uporabnikov, razen kadar je to zakonsko dovoljeno v skladu s členom 15(1). Ta odstavek ne preprečuje tehničnega shranjevanja, ki je potrebno za prenos sporočila, brez vpliva na načelo zaupnosti.

[…]

3. Države članice zagotovijo, da je shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika, dovoljeno samo pod pogojem, da je zadevni naročnik ali uporabnik v to privolil po tem, ko je bil jasno in izčrpno obveščen v skladu z Direktivo [95/46], med drugim o namenih obdelave. To ne prepreči nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja, ali, če je nujno potrebno, da ponudnik zagotovi storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata.“

7. Člen 6 Direktive 2002/58, naslovljen „Podatki o prometu“, določa:

„1. Podatki o prometu, ki se nanašajo na naročnike in uporabnike in ki jih je ponudnik javnega komunikacijskega omrežja ali javno razpoložljive elektronske komunikacijske storitve obdelal in shranil, morajo biti izbrisani ali predelani v anonimne, potem ko niso več potrebni za namen prenosa sporočila, kar ne vpliva na odstavke 2, 3 in 5 tega člena in člena 15(1).

2. Podatki o prometu, potrebni za namene zaračunavanja naročnikom in plačil za medsebojne povezave, se lahko obdelujejo. Taka obdelava je dovoljena samo do poteka obdobja, med katerim se lahko obračun zakonito izpodbija ali sprožijo postopki za pridobitev plačila.

[…]“

8. Člen 15 Direktive 2002/58, naslovljen „Uporaba nekaterih določb Direktive [95/46]“, v odstavku 1 določa:

„Države članice lahko sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9 te direktive, kadar takšna omejitev pomeni potreben, primeren in ustrezen ukrep znotraj demokratične družbe za zaščito državne [nacionalne] varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive [95/46]. V ta namen lahko države članice med

drugim sprejmejo zakonske ukrepe, ki določajo zadrževanje podatkov za določeno obdobje, upravičeno iz razlogov iz tega odstavka. Vsi ukrepi iz tega odstavka so v skladu s splošnimi načeli zakonodaje [Unije], vključno s tistimi iz člena 6(1) in (2) [PEU].“

B. Francosko pravo

1. Code de la propriété intellectuelle (zakonik o intelektualni lastnini)

9. Člen L. 331-12 code de la propriété intellectuelle (zakonik o intelektualni lastnini) v različici, ki se uporablja za spor o glavni stvari (v nadaljevanju: CPI), določa:

„Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Visoka oblast za razširjanje del in varstvo pravic na spletu, v nadaljevanju: Hadopi) je neodvisen javni organ.“

10. Člen L. 331-13 CPI določa:

„[Hadopi] zagotavlja:

[…]

2. nalogo varstva [del in predmetov, varovanih z avtorsko ali sorodnimi pravicami v elektronskih komunikacijskih omrežjih,] pred kršitvami teh pravic, storjenimi v elektronskih komunikacijskih omrežjih, ki se uporabljajo za zagotavljanje javnih spletnih komunikacijskih storitev; […]“

11. Člen L. 331-15 tega zakonika določa:

„[Hadopi] je sestavljena iz kolegija in komisije za varstvo pravic. […]

[…]

Člani kolegija in komisije za varstvo pravic pri izvrševanju svojih pristojnosti ne prejemajo navodil nobenega organa.“

12. Člen L. 331-17 navedenega zakonika določa:

„Komisija za varstvo pravic je pristojna za sprejemanje ukrepov iz člena L. 331-25.“

13. Člen L. 331-21 istega zakonika določa:

„Za izvrševanje pristojnosti komisije za varstvo pravic ima [Hadopi] na voljo zaprisežene javne uslužbence, ki jih pooblasti [njen] predsednik pod pogoji, ki so določeni z odlokom na podlagi mnenja Conseil d’État (državni svet). […]

Članom komisije za varstvo pravic in uslužbencem iz prvega odstavka se predložijo zadeve, ki so na navedeno komisijo naslovljene pod pogoji iz člena L 331-24. Njihova naloga je preučitev dejanskega stanja.

Za potrebe postopka lahko pridobijo vse dokumente, ne glede na njihov nosilec, vključno s podatki, ki jih hranijo in obdelujejo operaterji elektronskih komunikacij na podlagi člena L. 34-1 code des postes et des communications électroniques (zakonik o pošti in elektronskih komunikacijah) ter ponudniki storitev, navedeni v odstavkih 1 in 2 člena 6(I) loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (zakon št. 2004–575 z dne 21. junija 2004 o zaupanju v digitalno gospodarstvo).

Pridobijo lahko tudi kopije dokumentov, navedenih v prejšnjem odstavku.

Zlasti lahko od operaterjev elektronskih komunikacij pridobijo informacije o identiteti, poštnem naslovu, elektronskem naslovu in telefonski številki naročnika, čigar dostop do javnih spletnih komunikacijskih storitev je bil uporabljen za reproduciranje, predstavitev, dajanje na voljo ali priobčitev varovanih del ali predmetov javnosti brez dovoljenja imetnikov pravic […], kadar se tako dovoljenje zahteva."

14. Člen L. 331-24 CPI določa:

„Komisiji za varstvo pravic zadeve v obravnavo predložijo pooblaščeni zapriseženi uslužbenci […], ki jih imenujejo:

– poklicna telesa, ustanovljena v skladu s predpisi;

– organizacije za kolektivno upravljanje pravic;

– državni center za kinematografijo in animirano podobo.

Komisija za varstvo pravic lahko ukrepa tudi na podlagi informacij, ki ji jih predloži Procureur de la République (državni tožilec, Francija).

Ni ji mogoče predložiti zadev v zvezi z dejanji, starejšimi od šestih mesecev."

15. Člen L. 331-25 tega zakonika, ki ureja tako imenovani postopek „postopnega odgovora", določa:

„Kadar je komisiji za varstvo pravic predložena zadeva v zvezi z dejanji, ki bi lahko pomenila kršitev obveznosti, opredeljene v členu L. 336-3 [CPI], lahko naročniku pošlje […] priporočilo, v katerem ga opozori na določbe člena L. 336-3, mu odredi spoštovanje v njih opredeljene obveznosti in ga opozori na sankcije, zagrožene v skladu s členoma L. 335-7 in L. 335-7-1. To priporočilo vsebuje tudi informacijo naročniku o zakoniti ponudbi spletnih kulturnih vsebin, o obstoju sredstev za zavarovanje, s katerimi je mogoče preprečiti kršitve obveznosti, opredeljene v členu L. 336-3, ter o nevarnostih, ki jih za nadaljnje umetniško ustvarjanje in ekonomijo kulturnega sektorja pomenijo prakse, s katerimi se ne spoštujejo avtorska in sorodne pravice.

Če se v šestih mesecih od pošiljanja priporočila iz prvega odstavka dejanja, ki bi lahko pomenila kršitev obveznosti, opredeljene v členu L. 336-3, ponovijo, lahko komisija po elektronski poti pošlje novo priporočilo, ki vsebuje enake informacije kot prejšnje […]. To priporočilo mora poslati skupaj s priporočenim dopisom ali na kakršen koli drug način, s katerim se lahko dokaže datum vročitve tega priporočila.

V priporočilih, poslanih na podlagi tega člena, sta navedena datum in ura, ko so bila ugotovljena dejanja, ki bi lahko pomenila kršitev obveznosti, opredeljene v členu L. 336-3. Nasprotno pa se v njih ne razkrije vsebina varovanih del ali predmetov, na katere se ta kršitev nanaša. V njih so navedeni telefonska številka ter poštni in elektronski naslov, prek katerih lahko njihov naslovnik, če to želi, komisiji za varstvo pravic predloži pripombe in, če to izrecno zahteva, pridobi pojasnila o vsebini varovanih del ali predmetov, na katere se nanaša kršitev, ki se mu očita.“

16. Člen L. 331-29 navedenega zakonika določa:

„[Hadopi] sme vzpostaviti avtomatsko obdelavo osebnih podatkov posameznikov, proti katerim je uveden postopek v okviru tega pododdelka.

Namen te obdelave je omogočiti, da komisija za varstvo pravic izvaja ukrepe, določene v tem pododdelku, vse z njimi povezane procesne akte in podrobna pravila o obveščanju poklicnih teles in organizacij za upravljanje avtorskih pravic o morebitnih sodnih postopkih ter vročitvah, določenih v petem odstavku člena L. 335-7.

[…] z odlokom [se] opredeli[jo] način[i] izvajanja tega člena. Z odlokom se zlasti določijo:

– kategorije hranjenih podatkov in obdobje njihove hrambe;

– naslovniki, ki so upravičeni do prejema teh podatkov, zlasti osebe, katerih dejavnost je zagotavljanje dostopa do storitev javnih spletnih komunikacijskih storitev;

– pogoji, pod katerimi lahko zainteresirane osebe pri [Hadopi] uveljavljajo svojo pravico do dostopa do podatkov, ki se nanašajo nanje […]“

17. Člen R. 331-37 istega zakonika določa:

„Operaterji elektronskih komunikacij […] in ponudniki storitev […] so zavezani, da prek povezave s sistemom za avtomatsko obdelavo osebnih podatkov iz člena L. 331-29 ali z uporabo nosilca za snemanje, ki zagotavlja njihovo integriteto in varnost, posredujejo osebne podatke in informacije, navedene v točki 2 priloge k [décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du [CPI] dénommé ‚Système de gestion des mesures pour la protection des œuvres sur Internet‘ (odlok št. 2010-236 z dne 5. marca 2010 o avtomatizirani obdelavi osebnih podatkov, ki je dovoljena s členom L. 331-29 zakonika o intelektualni lastnini in ki je imenovana „Sistem upravljanja ukrepov za varstvo del na spletu“ [4])] […], v osmih dneh po tem, ko je komisija za varstvo pravic posredovala tehnične podatke, potrebne za identifikacijo naročnika, čigar dostop do podatkov o javnih spletnih komunikacijah je bil uporabljen za reproduciranje, predstavitev, dajanje na voljo ali priobčitev varovanih del ali predmetov javnosti brez dovoljenja imetnikov pravic […], kadar se to dovoljenje zahteva.

[…]“

[4] JORF z dne 7. marca 2010, besedilo št. 19.

18. Člen R. 335-5 CPI določa:

„I. Resno malomarnost, ki se kaznuje z globo, določeno za prekrške pete stopnje, pomeni dejstvo, da imetnik dostopa do javnih spletnih komunikacijskih storitev brez upravičenega razloga in če so izpolnjeni pogoji, določeni v odstavku II:

1. bodisi ni vzpostavil sredstva za zavarovanje tega dostopa

2. bodisi ni izkazal zadostne skrbnosti pri uporabi tega sredstva.

II. Določbe odstavka I se uporabljajo le, če sta izpolnjena oba spodaj navedena pogoja:

1. komisija za varstvo pravic je v skladu s členom L. 331-25 in na način, določen v tem členu, imetniku dostopa priporočila, naj uporabi sredstvo za zavarovanje svojega dostopa, s katerim bo mogoče preprečiti ponovno uporabo tega dostopa za reproduciranje, predstavitev, dajanje na voljo ali priobčitev javnosti del, varovanih z avtorsko ali sorodnimi pravicami, brez dovoljenja imetnikov teh pravic […], kadar se to dovoljenje zahteva;

2. v enem letu po predložitvi tega priporočila se ta dostop znova uporabi za namene, navedene v točki 1 tega odstavka II.“

19. Člen L. 336-3 tega zakonika določa:

„Imetnik dostopa do javnih spletnih komunikacijskih storitev mora zagotavljati, da se ta dostop ne uporablja za reproduciranje, predstavitev, dajanje na voljo ali priobčitev javnosti del, varovanih z avtorsko ali sorodnimi pravicami, brez dovoljenja imetnikov[…], kadar se to dovoljenje zahteva.

Če imetnik dostopa krši obveznost, opredeljeno v prvem odstavku, za zadevno osebo ne nastane kazenska odgovornost […]“

2. Décret du 5 mars 2010 (odlok z dne 5. marca 2010)

20. Odlok z dne 5. marca 2010 v različici, ki se uporablja za dejansko stanje v sporu o glavni stvari, v členu 1 določa:

„Namen obdelave osebnih podatkov, poimenovane ‚Sistem upravljanja ukrepov za varstvo del na spletu‘, je komisiji za varstvo pravic pri [Hadopi] omogočiti:

1. izvajanje ukrepov, določenih v knjigi III zakonodajnega dela [CPI] (naslov III, poglavje I, oddelek 3, pododdelek 3) in knjigi III uredbenega dela istega zakonika (naslov III, poglavje I, oddelek 2, pododdelek 2);

2. obravnavo zadev, ki jih predloži državni tožilec v zvezi z dejanji, ki bi lahko pomenila kršitev členov L. 335-2, L. 335-3, L. 335-4 in R. 335-5 istega zakonika, ter obveščanje poklicnih teles in organizacij za kolektivno upravljanje o tem, da so bile navedene zadeve predložene;

[…]“

21. Člen 4 tega odloka določa:

„I.- Neposreden dostop do osebnih podatkov in informacij, navedenih v prilogi k temu odloku, imajo zapriseženi javni uslužbenci, ki jih pooblasti predsednik [Hadopi] v skladu s členom L. 331-21 [CPI], in člani komisije za varstvo pravic, navedene v členu 1.

II.- Operaterjem elektronskih komunikacij in ponudnikom storitev, navedenim v točki 2 priloge k temu odloku, so predloženi:

– tehnični podatki, potrebni za identifikacijo naročnika;

– priporočila iz člena L. 331-25 [CPI], da zagotovijo njihovo pošiljanje svojim naročnikom po elektronski poti;

– elementi, potrebni za izvršitev dopolnilnih kazni začasne ukinitve dostopa do javne spletne komunikacijske storitve, s katerimi komisijo za varstvo pravic seznani državni tožilec.

III.- Poklicna telesa in organizacije za kolektivno upravljanje so obveščeni o zadevah, ki jih je predložil državni tožilec.

IV.- Pravosodnim organom so predloženi zapisniki o ugotovitvi dejanj, ki bi lahko pomenila kršitve, določene s členi L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 in R. 335-5 [CPI].

Informacija o izvršitvi kazni začasne ukinitve dostopa se vnese v avtomatizirano kazensko evidenco.“

22. Priloga k odloku z dne 5. marca 2010 določa:

„Osebni podatki in informacije, ki se hranijo v sistemu obdelave, poimenovanem ‚Sistem upravljanja ukrepov za varstvo del na spletu‘, so:

1. osebni podatki in informacije, katerih vir so poklicna telesa, ustanovljena v skladu s predpisi, organizacije za kolektivno upravljanje, državni center za kinematografijo in animirano podobo ter državni tožilec:

v zvezi z dejanji, ki bi lahko pomenila kršitev obveznosti, opredeljene v členu L. 336-3 [CPI]:

datum in ura storitve dejanj;

IP-naslov zadevnih naročnikov;

uporabljeni protokol P2P;

psevdonim, ki ga uporablja naročnik;

informacije o varovanih delih ali predmetih, na katere se nanašajo storjena dejanja;

ime datoteke, kot je navedeno na naročnikovi terminalni opremi (če je to primerno);

ponudnik dostopa do spleta, pri katerem je bil sklenjen dostop ali ki je zagotovil tehnični vir IP. […]

2. osebni podatki in informacije o naročniku, zbrani pri operaterjih elektronskih komunikacij […] in ponudnikih […]:

priimek, imena;

poštni naslov in e-poštni naslovi;

telefonska številka;

naslov naročnikove telefonske naprave;

ponudnik dostopa do spleta, ki uporablja tehnične vire ponudnika dostopa, navedenega v točki 1, pri katerem je naročnik sklenil pogodbo; številka spisa;

datum začetka začasne ukinitve dostopa do javne spletne komunikacijske storitve.

[…]“

3. Code des postes et des télécommunications (zakonik o pošti in telekomunikacijah)

23. Člen L. 34-1 code des postes et des communications électroniques (zakonik o pošti in elektronskih komunikacijah), kakor je bil spremenjen s členom 17 loi n° 2021-998 du 30 juillet 2021 [5] (zakon št. 2021-998 z dne 30. julija 2021, v nadaljevanju: CPCE), v odstavku IIa določa, da „[o]peraterji elektronskih komunikacij hranijo:

1. za potrebe kazenskih postopkov, preprečevanja groženj javni varnosti in zaščite nacionalne varnosti informacije o civilni identiteti uporabnika pet let po izteku veljavnosti njegove pogodbe;

2. za enake namene, kot so navedeni v točki 1 tega odstavka IIa, druge informacije, ki jih predloži uporabnik, ko sklene pogodbo ali ustvari račun, in informacije o plačilu eno leto po izteku veljavnosti njegove pogodbe ali zaprtju računa;

3. za potrebe boja proti kriminalu in hudim kaznivim dejanjem, preprečevanja resnih groženj javni varnosti in zaščite nacionalne varnosti tehnične podatke, na podlagi katerih je mogoče identificirati vir povezave, ali podatke v zvezi z uporabljeno terminalsko opremo eno leto po povezavi ali uporabi terminalske opreme.“

[5] JORF z dne 31. julija 2021, besedilo št. 1. Ta različica člena L. 34-1 CPCE, ki velja od 31. julija 2021, je bila sprejeta po izdaji odločbe Conseil d'État (državni svet, Francija) z dne 21. aprila 2021, št. 393099 (JORF z dne 25. aprila 2021), s čimer je bila razveljavljena predhodna različica te določbe, ki je vsebovala obveznost hrambe osebnih podatkov „za potrebe preiskovanja, ugotavljanja in pregona kaznivih dejanj ali neizpolnitve obveznosti, opredeljene v členu L. 336-3 [CPI]“, in sicer zgolj zato, da se lahko po potrebi dajo na voljo zlasti Hadopi. Conseil constitutionnel (ustavni svet, Francija) je z odločbo št. 2021-976-977 QPC z dne 25. februarja 2022 (Habib A. in drugi) odločil, da je navedena prejšnja različica člena L. 34-1 CPCE protiustavna, pri čemer je kot bistveni razlog navedel, da „je z izpodbijanimi določbami, ker se z njimi dovoljuje splošna in neselektivna hramba podatkov o povezavi, nesorazmerno poseženo v pravico do spoštovanja zasebnega življenja“ (točka 13). To sodišče je namreč menilo, da se podatki o povezavi, ki jih je treba hraniti v skladu s temi določbami, nanašajo ne samo na identifikacijo uporabnikov elektronskih komunikacijskih storitev, ampak tudi na druge podatke, ki „glede na njihovo raznolikost in to, kako se lahko obdelujejo, o teh uporabnikih in po potrebi tretjih osebah zagotavljajo številne natančne informacije, kar pomeni posebej hud poseg v njihovo zasebno življenje“ (točka 11).

III. Spor o glavni stvari, vprašanja za predhodno odločanje in postopek pred Sodiščem

24. La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net in French Data Network so s tožbo z dne 12. avgusta 2019 in dvema dopolnilnima vlogama z dne 12. novembra 2019 in 6. maja 2021 pri Conseil d'État (državni svet, Francija) vložili predlog za odpravo odločbe na podlagi molka organa, s katero je Premier ministre (predsednik vlade) zavrnil njihov predlog za razveljavitev odloka z dne 5. marca 2010, čeprav naj bi bilo s tem odlokom in določbami, ki tvorijo njegovo zakonsko podlago, ne samo prekomerno poseženo v pravice, zagotovljene s francosko ustavo, ampak naj bi bili poleg tega tudi v nasprotju s členom 15 Direktive 2002/58 ter členi 7, 8, 11 in 52 Listine.

25. Natančneje, tožeče stranke iz postopka v glavni stvari trdijo, da je z odlokom z dne 5. marca 2010 in določbami, ki tvorijo njegovo zakonsko podlago, dovoljen nesorazmeren dostop do podatkov o povezavi za manjše kršitve v zvezi z avtorsko pravico, storjene na spletu, brez predhodnega nadzora sodišča ali organa, katerega neodvisnost in nepristranskost sta zajamčeni.

26. Predložitveno sodišče v zvezi s tem najprej poudarja, da je Sodišče v zadnji sodbi La Quadrature du Net in drugi [6] razsodilo, da člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8, 11 in 52(1) Listine ne nasprotuje zakonskim ukrepom, s katerimi je za zaščito nacionalne varnosti, boj proti kriminalu in zaščito javne varnosti določena splošna in neselektivna hramba *podatkov o civilni identiteti* uporabnikov elektronskih komunikacijskih sredstev. Tako naj bi bila taka hramba podatkov mogoča brez posebnega roka za preiskovanje, odkrivanje in pregon kaznivih dejanj na splošno.

27. Predložitveno sodišče na podlagi tega ugotavlja, da je treba tožbeni razlog, ki so ga tožeče stranke uveljavljale v postopku v glavni stvari in se nanaša na nezakonitost odloka z dne 5. marca 2010, ker je bil sprejet v okviru boja proti kaznivim dejanjem, ki niso posebej huda, zavrniti.

28. To sodišče nato opozarja, da je Sodišče v sodbi Tele2 Sverige in Watson [7] razsodilo, da je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8, 11 in 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki ureja varstvo in varnost podatkov o prometu in podatkov o lokaciji ter zlasti dostop pristojnih nacionalnih organov do hranjenih podatkov, pri čemer ni določeno, da mora nadzor nad navedenim dostopom predhodno opraviti sodišče ali neodvisen upravni organ.

29. Poudarja, da je Sodišče v sodbi Tele2 [8] pojasnilo, da je za to, da se v praksi zagotovi popolno spoštovanje teh pogojev, bistveno, da je dostop pristojnih nacionalnih organov do hranjenih podatkov načeloma, razen v nujnih primerih, ki so ustrezno utemeljeni, pogojen z zahtevo, da sodišče ali neodvisen upravni organ opravi predhodni nadzor in da se odločba tega sodišča ali tega organa izda na obrazložen predlog, ki se predloži v postopku preprečevanja, odkrivanja ali pregona kaznivih dejanj.

6 Glej sodbo z dne 6. oktobra 2020 (C-511/18, C-512/18 in C-520/18, v nadaljevanju: sodba Quadrature du Net in drugi, EU:C:2020:791, izrek).

7 Glej sodbo z dne 21. decembra 2016 (C-203/15 in C-698/15, v nadaljevanju: sodba Tele2, EU:C:2016:970, izrek).

8 Točka 120 te sodbe.

30. Predložitveno sodišče poudarja, da je Sodišče to zahtevo ponovilo v sodbi La Quadrature du Net in drugi [9] v zvezi z zbiranjem podatkov o povezavah s strani obveščevalnih služb v realnem času ter v sodbi Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah) [10] v zvezi z dostopom nacionalnih organov do podatkov o povezavah.

31. To sodišče nazadnje ugotavlja, da je Hadopi od ustanovitve leta 2009 na imetnike naročnin naslovila več kot 12,7 milijona priporočil v skladu s postopkom postopnega odgovora, določenim s členom L. 331-25 CPI, od tega 827.791 samo v letu 2019. Za to morajo uslužbenci komisije za varstvo pravic pri Hadopi vsako leto zbrati ogromno število podatkov o civilni identiteti zadevnih uporabnikov. Če bi bilo to zbiranje podatkov predmet predhodnega nadzora, po mnenju tega sodišča izdaja priporočil glede na njihov obseg ne bi bila mogoča.

32. V teh okoliščinah je Conseil d'État (državni svet) prekinil odločanje in Sodišču v predhodno odločanje predložil ta vprašanja:

„1. Ali so podatki o civilni identiteti, ki ustrezajo IP-naslovu, vključeni med podatke o prometu ali o lokaciji, ki morajo biti načeloma predmet predhodnega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločbe so zavezujoče?

2. Če je odgovor na prvo vprašanje pritrdilen in ob upoštevanju nizke občutljivosti podatkov o osebni identiteti uporabnikov, vključno z njihovimi kontaktnimi podatki, ali je treba Direktivo [2002/58] v povezavi z [Listino] razlagati tako, da nasprotuje nacionalni ureditvi, v skladu s katero upravni organ zbira te podatke, ki ustrezajo IP-naslovu uporabnikov, brez predhodnega nadzora sodišča ali neodvisnega upravnega organa, katerega odločbe so zavezujoče?

3. Če je odgovor na drugo vprašanje pritrdilen in ob upoštevanju nizke občutljivosti podatkov o civilni identiteti in okoliščine, da se lahko zgolj ti podatki zbirajo samo za namene preprečevanja kršitev obveznosti, ki so z nacionalnim pravom natančno, omejeno in omejevalno določene, ter okoliščine, da bi sistematičen nadzor nad dostopom do podatkov vsakega uporabnika, ki ga opravi sodišče ali tretji upravni organ, katerega odločbe so zavezujoče, lahko ogrozil izpolnjevanje naloge javne službe, ki je zaupana prav tako neodvisnemu upravnemu organu, ki zbira te podatke, ali Direktiva [2002/58] nasprotuje temu, da se ta nadzor opravlja na prilagojen način, na primer v obliki avtomatiziranega nadzora, po potrebi s pregledom interne službe organa, katerega neodvisnost in nepristranskost je zajamčena v razmerju do uradnikov, ki so zadolženi za nalogo zbiranja podatkov?“

33. Pisna stališča so predložile tožeče stranke v postopku v glavni stvari, francoska, estonska, švedska in norveška vlada ter Evropska komisija. Iste stranke, razen estonske, danske in finske vlade, so bile zastopane na obravnavi 5. julija 2022.

[9] Točka 189 te sodbe.

[10] Sodba z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah) (C-746/18, v nadaljevanju: sodba Prokuratuur, EU:C:2021:152).

IV. Analiza

A. Prvo in drugo vprašanje za predhodno odločanje

34. Predložitveno sodišče želi s prvim in drugim vprašanjem za predhodno odločanje, ki ju je treba po mojem mnenju preučiti skupaj, v bistvu izvedeti, ali je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki upravnemu organu, pristojnemu za varstvo avtorske in sorodnih pravic pred kršitvami teh pravic, storjenimi na spletu, omogoča dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, zato da lahko ta organ identificira imetnike teh naslovov, v zvezi s katerimi je podan sum, da so odgovorni za te kršitve, in lahko po potrebi v zvezi z njimi sprejme ukrepe brez predhodnega nadzora sodišča ali neodvisnega upravnega organa.

1. Razmejitev vprašanj za predhodno odločanje

a) Predhodno zbiranje IP-naslovov s strani organizacij imetnikov pravic

35. Iz predložitvene odločbe je razvidno, da mehanizem postopnega odgovora iz postopka v glavni stvari zajema dve zaporedni obdelavi podatkov, pri čemer v okviru prve predhodno zbiranje IP-naslovov opravijo organizacije imetnikov pravic v omrežjih P2P kršiteljev avtorske pravice, v okviru druge pa Hadopi te IP-naslove poveže s civilno identiteto oseb, potem ko ji je bila zadeva predložena, da pošlje priporočila osebam, katerih dostop do javnih spletnih komunikacijskih storitev je bil uporabljen v nasprotju s pravili glede avtorskih pravic.

36. Prvo in drugo vprašanje za predhodno odločanje se nanašata zgolj na drugo obdelavo, ki jo opravi Hadopi.

37. Vendar tožeče stranke iz postopka v glavni stvari trdijo, da bi moralo Sodišče preučiti prvo obdelavo, saj naj bi bila uporaba teh IP-naslovov v okviru druge obdelave, če so bili ti naslovi pridobljeni v nasprotju z določbami Direktive 2002/58, nujno v nasprotju s temi določbami.

38. Takšno razlogovanje ne prepriča. Člen 3(1) Direktive 2002/58 omejuje njeno področje uporabe na „obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev“. Kot pa je na obravnavi pojasnila francoska vlada, organizacije imetnikov pravic zadevnih IP-naslovov ne pridobijo od ponudnikov elektronskih komunikacijskih storitev, ampak neposredno na spletu z vpogledom v podatke, ki so na voljo širši javnosti.

39. Torej je mogoče zgolj ugotoviti, da se za predhodno zbiranje IP-naslovov, ki ga opravijo organizacije imetnikov pravic, ne uporabljajo določbe Direktive 2002/58 in da bi ga bilo torej mogoče, kot navaja Komisija, analizirati z vidika določb Uredbe (EU) 2016/679.[11] Zato menim, da taka analiza presega okvir vprašanj za predhodno odločanje, postavljenih Sodišču, in sicer še toliko bolj, ker predložitveno sodišče ni predložilo pojasnil v zvezi s predhodnim zbiranjem, ki bi Sodišču omogočila, da mu koristno odgovori.

[11] Uredba Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL 2016, L 119, str. 1, popravek v UL 2018, L 127, str. 2).

40. V teh okoliščinah se bom pri analizi osredotočil na vprašanje dostopa, ki ga ima Hadopi do podatkov o civilni identiteti, ki ustrezajo IP-naslovu.

b) Povezava IP-naslovov s podatki o civilni identiteti

41. Prvo in drugo vprašanje za predhodno odločanje se nanašata na „podatke o civilni identiteti, ki ustrezajo IP-naslovu“ in ki so po mnenju predložitvenega sodišča podatki nizke občutljivosti. To sodišče se v svoji odločbi sklicuje izključno na točke sodbe La Quadrature du Net in drugi, ki se nanašajo na hrambo podatkov o civilni identiteti.

42. Drži sicer, da Sodišče v svoji sodni praksi razlikuje med ureditvijo hrambe IP-naslovov in dostopa do njih ter ureditvijo hrambe podatkov v zvezi s civilno identiteto uporabnikov elektronskih komunikacijskih sredstev in dostopa do njih, pri čemer je druga ureditev manj stroga od prve. [12]

43. Vendar se mi zdi, da v obravnavani zadevi kljub taki formulaciji teh dveh vprašanj za predhodno odločanje ne gre za vprašanje samo dostopa do podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev, ampak za povezavo teh podatkov z IP-naslovi, ki so na voljo Hadopi, potem ko so jih organizacije imetnikov pravic zbrale in jih posredovale. Kot namreč navaja Komisija, je namen dostopa do podatkov o civilni identiteti, ki ga ima Hadopi, deblokirati širši sklop podatkov, zlasti IP-naslovov in izvlečkov ogledanih datotek, ter omogočiti njihovo uporabo, pri čemer podatki o civilni identiteti in IP-naslovi neodvisno drugi od drugih za nacionalne organe niso zanimivi, saj niti civilna identiteta niti IP-naslov sam zase ne moreta zagotoviti informacij o spletnih dejavnostih fizičnih oseb, če se ta podatka med seboj ne povežeta.

44. Iz tega sledi, da je treba po mojem mnenju prvo in drugo vprašanje za predhodno odločanje razumeti tako, da se ne nanašata samo na podatke o civilni identiteti uporabnikov elektronskega komunikacijskega sredstva, ampak tudi na dostop do IP-naslovov, ki omogoča identifikacijo vira povezave.

c) Hramba IP-naslovov s strani ponudnikov komunikacijskih storitev

45. Kot ugotavljata francoska vlada in Komisija, sicer drži, da se vprašanja za predhodno odločanje, postavljena Sodišču, formalno ne nanašajo na hrambo podatkov s strani ponudnikov elektronskih komunikacijskih storitev, ampak samo na dostop, ki ga ima Hadopi do podatkov o civilni identiteti, ki ustrezajo IP-naslovom.

46. Vendar menim, da je vprašanje dostopa Hadopi do teh podatkov dejansko neločljivo povezano s predhodnim vprašanjem njihove hrambe s strani ponudnikov komunikacijskih storitev. Kot je poudarilo Sodišče, so podatki hranjeni le za to, da se – če je to potrebno – pristojnim nacionalnim organom omogoči dostop do njih. [13] Povedano drugače, hrambe podatkov in dostopa do njih ni mogoče zasnovati ločeno, saj je drugi odvisen od prve.

[12] Glej sodbo La Quadrature du Net in drugi (točki 155 in 159).

[13] Glej sodbo Tele2 (točka 79).

47. Drži sicer, da je Sodišče že preučilo, ali je s členom 15(1) Direktive 2002/58 združljiva nacionalna ureditev, ki se je nanašala samo na dostop pristojnih nacionalnih organov do nekaterih osebnih podatkov, neodvisno od vprašanja, ali je s to določbo združljiva hramba zadevnih podatkov.[14] Torej bi bilo mogoče na ta vprašanja za predhodno odločanje odgovoriti brez obravnave vprašanja, ali so bili zadevni podatki hranjeni v skladu z določbami prava Unije.

48. Vendar najprej ugotavljam, da se pri preučitvi, ki jo je Sodišče opravilo v sodbi Ministerio Fiscal[15], kar zadeva združljivost dostopa nacionalnih organov do nekaterih osebnih podatkov s pravom Unije, uporabljajo povsem enaka načela kot pri preučitvi, ki jo opravi v zvezi s presojo združljivosti hrambe teh podatkov s pravom Unije. Sodišče namreč napotuje izključno na sodno prakso, izoblikovano v zvezi z zadnjenavedenim vidikom, ki jo je preneslo na vprašanje dostopa do osebnih podatkov. Povedano drugače, če združljivost hrambe nekaterih podatkov s pravom Unije ni preučena, se ta preučitev prenese v fazo vprašanja dostopa do teh podatkov, tako da je združljivost tega dostopa navsezadnje odvisna od združljivosti hrambe.

49. Dalje, Sodišče je jasno navedlo, da je mogoče dostop do osebnih podatkov dovoliti le, če so ponudniki elektronskih komunikacijskih storitev te podatke hranili na način, ki je v skladu s členom 15(1) Direktive 2002/58[16], in da je dostop oseb zasebnega prava do osebnih podatkov, zato da se jim tako omogoči vložitev odškodninske tožbe pred civilnimi sodišči zaradi kršitev avtorske pravice, s pravom Unije združljiv le, če so bili ti podatki hranjeni na način, združljiv s to določbo[17].

50. Nazadnje, Sodišče dosledno razsoja, da je dostop do podatkov o prometu in podatkov o lokaciji, ki jih hranijo ponudniki na podlagi ukrepa, sprejetega na podlagi člena 15(1) Direktive 2002/58, ki ga je treba izvesti ob polnem spoštovanju pogojev, ki izhajajo iz sodne prakse, s katero je bila podana razlaga Direktive 2002/58, načeloma mogoče upravičiti le s ciljem v splošnem interesu, za katerega je bila ta hramba naložena tem ponudnikom.[18] Povedano drugače, združljivost dostopa nacionalnih organov do nekaterih osebnih podatkov s pravom Unije je v celoti odvisna od združljivosti hrambe teh podatkov s pravom Unije.

51. Iz tega po mojem mnenju izhaja, da je treba pred analizo združljivosti nacionalne ureditve, ki določa dostop nacionalnega organa do osebnih podatkov, ugotoviti združljivost hrambe istih podatkov s pravom Unije.

52. V teh okoliščinah bom analizo začel s pregledom sodne prakse Sodišča v zvezi z vprašanjem hrambe IP-naslovov, dodeljenih viru povezave, da bom tako pokazal njene omejitve in nato predlagal okvir za ustrezno prilagojeno razumevanje zadevne ureditve.

14 Glej sodbo z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točka 49).

15 Sodba z dne 2. oktobra 2018 (C-207/16, EU:C:2018:788).

16 Glej sodbo Prokuratuur (točka 29).

17 Glej sodbo z dne 17. junija 2021, M.I.C.M. (C-597/19, EU:C:2021:492, točke od 127 do 130).

18 Glej sodbe La Quadrature du Net in drugi, točka 166; z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi (C-140/20, v nadaljevanju: sodba Commissioner of An Garda Síochána in drugi, EU:C:2022:258, točka 98), in z dne 20. septembra 2022, SpaceNet (C-793/19 in C-794/19, v nadaljevanju: sodba SpaceNet, EU:C:2002:702, točka 131).

2. Sodna praksa Sodišča v zvezi z razlago člena 15(1) Direktive 2002/58/ES glede ukrepov za hrambo IP-naslovov, dodeljenih viru povezave

53. Člen 5(1) Direktive 2002/58 določa načelo zaupnosti elektronskih komunikacij in z njimi povezanih podatkov o prometu ter med drugim zahteva, da se načeloma vsem, razen uporabnikom, prepove shranjevanje teh komunikacij in podatkov brez privolitve uporabnikov. [19]

54. Direktiva 2002/58 glede obdelave in shranjevanja podatkov o prometu, ki se nanašajo na naročnike in uporabnike, s strani ponudnikov elektronskih komunikacijskih storitev v členu 6(1) določa, da morajo biti ti podatki izbrisani ali predelani v anonimne, potem ko niso več potrebni za prenos sporočila, v členu 6(2) pa določa, da se podatki o prometu, potrebni za namene zaračunavanja naročnikom in plačil za medsebojne povezave lahko obdelujejo le do poteka obdobja, med katerim se lahko obračun zakonito izpodbija ali med katerim se lahko sprožijo postopki za pridobitev plačila. Glede podatkov o lokaciji, ki niso podatki o prometu, člen 9(1) te direktive določa, da se smejo takšni podatki obdelati le pod določenimi pogoji in šele po tem, ko postanejo anonimni, ali s privolitvijo uporabnikov ali naročnikov. [20]

55. Zakonodajalec Unije je tako s sprejetjem Direktive 2002/58 konkretiziral pravice, določene v členih 7 in 8 Listine, tako da so uporabniki elektronskih komunikacijskih sredstev načeloma upravičeni pričakovati, da bodo njihova sporočila in z njimi povezani podatki, če ne privolijo v nasprotno, ostali anonimni in jih ne bo mogoče shraniti. [21] Ta direktiva zato ni omejena na to, da dostop do takih podatkov ureja z zaščitnimi ukrepi, katerih namen je preprečevanje zlorab, temveč zlasti določa tudi načelo prepovedi njihovega shranjevanja s strani tretjih oseb.

56. V teh okoliščinah, ker člen 15(1) Direktive 2002/58 državam članicam omogoča, da sprejmejo zakonske ukrepe, katerih namen je „omejiti obseg“ pravic in obveznosti, določenih zlasti v členih 5, 6 in 9 te direktive, kot so tiste, ki izhajajo iz načel zaupnosti sporočil in prepovedi hrambe s tem povezanih podatkov, ta določba določa izjemo od splošnega pravila, določenega zlasti v teh členih 5, 6 in 9 te direktive, in jo je zato treba v skladu z ustaljeno sodno prakso razlagati ozko. Taka določba torej ne more upravičiti tega, da odstopanje od načelne obveznosti zagotavljanja zaupnosti elektronskih komunikacij in z njimi povezanih podatkov ter zlasti od prepovedi shranjevanja teh podatkov, ki je izrecno določena v členu 5 navedene direktive, postane pravilo, sicer bi se zadnjenavedeni določbi odvzel njen pomen. [22]

57. V zvezi s cilji, s katerimi je mogoče upravičiti omejitev pravic in obveznosti, določenih zlasti v členih 5, 6 in 9 Direktive 2002/58, je Sodišče že razsodilo, da je naštevanje ciljev iz člena 15(1), prvi stavek, te direktive izčrpno, tako da mora zakonski ukrep, sprejet na podlagi te določbe, dejansko in strogo ustrezati enemu od teh ciljev. [23]

58. Poleg tega je iz člena 15(1), tretji stavek, Direktive 2002/58 razvidno, da morajo ukrepi, ki jih države članice sprejmejo na podlagi te določbe, spoštovati splošna načela prava Unije, med katerimi je načelo sorazmernosti, in zagotoviti spoštovanje temeljnih pravic, zagotovljenih z Listino. V zvezi s tem je Sodišče že razsodilo, da se z obveznostjo, ki jo država članica

[19] Glej sodbe La Quadrature du Net in drugi (točka 107); Commissioner of An Garda Síochána in drugi (točka 35) in SpaceNet (točka 52).

[20] Glej sodbe Tele2 (točka 86); La Quadrature du Net in drugi (točka 108); Commissioner of An Garda Síochána in drugi (točka 38) in SpaceNet (točka 55).

[21] Glej sodbe La Quadrature du Net in drugi (točka 109); Commissioner of An Garda Síochána in drugi (točka 37) in SpaceNet (točka 54).

[22] Glej sodbe La Quadrature du Net in drugi (točki 110 in 111); Commissioner of An Garda Síochána in drugi (točka 40) in SpaceNet (točka 57).

[23] Glej sodbe La Quadrature du Net in drugi (točka 112); Commissioner of An Garda Síochána in drugi (točka 41) in SpaceNet (točka 58).

z nacionalno ureditvijo naloži ponudnikom elektronskih komunikacijskih storitev, da hranijo podatke o prometu, zato da se, če je to potrebno, pristojnim nacionalnim organom omogoči dostop do teh podatkov, postavljajo vprašanja v zvezi s spoštovanjem ne le členov 7 in 8 Listine, ki se nanašata na varstvo zasebnega življenja in varstvo osebnih podatkov, ampak tudi člena 11 Listine, ki se nanaša na svobodo izražanja, glede na to, da je ta svoboda eden od glavnih temeljev demokratične in pluralistične družbe ter je del vrednot, na katerih v skladu s členom 2 PEU temelji Unija. [24]

59. Ker pa člen 15(1) Direktive 2002/58 državam članicam dopušča, da omejijo pravice in obveznosti iz členov 5, 6 in 9 te direktive, se v tej določbi odraža dejstvo, da pravice iz členov 7, 8 in 11 Listine niso absolutne, temveč jih je treba upoštevati glede na njihovo funkcijo v družbi. Kot namreč izhaja iz člena 52(1) Listine, ta dopušča omejitve pri uresničevanju teh pravic, če so te omejitve predpisane z zakonom, če spoštujejo bistveno vsebino teh pravic, če so ob upoštevanju načela sorazmernosti potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali so potrebne zaradi zaščite pravic in svoboščin drugih. Tako razlaga člena 15(1) Direktive 2002/58 v povezavi z Listino zahteva tudi upoštevanje pomembnosti ciljev zaščite nacionalne varnosti in boja proti hudemu kriminalu, s čimer se pripomore k varstvu pravic in svoboščin drugih, ter pomembnosti pravic, določenih s členi 3, 4, 6 in 7 Listine [25], iz katerih lahko izhajajo pozitivne obveznosti za javne organe [26].

60. Ob upoštevanju teh različnih pozitivnih obveznosti je treba torej uskladiti različne zadevne legitimne interese in pravice. V tem okviru iz samega besedila člena 15(1), prvi stavek, Direktive 2002/58 izhaja, da lahko države članice sprejmejo ukrep, ki odstopa od načela zaupnosti, kadar je tak ukrep „potreben, primeren in ustrezen [sorazmeren] […] znotraj demokratične družbe“, pri čemer je v uvodni izjavi 11 te direktive navedeno, da mora biti tak ukrep „dosledno“ sorazmeren z zastavljenim ciljem. [27]

61. V zvezi s tem je iz sodne prakse Sodišča razvidno, da je treba možnost za države članice, da utemeljijo omejitev pravic in obveznosti, določenih zlasti s členi 5, 6 in 9 Direktive 2002/58, presojati tako, da se oceni teža posega, ki ga pomeni taka omejitev, in preveri, ali je pomembnost cilja splošnega interesa, ki se uresničuje s to omejitvijo, v sorazmerju s to težo. [28]

62. Naj k temu še dodam, da Sodišče v svoji sodni praksi razlikuje med na eni strani posegi, ki izhajajo iz dostopa do podatkov in že sami po sebi zagotavljajo natančne informacije o zadevnih komunikacijah in torej o zasebnem življenju osebe, zato je zanje ureditev hrambe stroga, ter na drugi strani posegi, ki izhajajo iz dostopa do podatkov, iz katerih je mogoče take informacije pridobiti le, če se povežejo z drugimi podatki, kot so IP-naslovi. [29]

63. Natančneje, Sodišče je v zvezi z IP-naslovi ugotovilo, da se ti ustvarijo, ne da bi bili vezani na določeno komunikacijo, služijo pa predvsem temu, da se prek ponudnikov elektronskih komunikacijskih storitev identificira fizična oseba, ki je lastnik terminalske opreme, s katere je

[24] Glej sodbe La Quadrature du Net in drugi (točki 113 in 114); Commissioner of An Garda Síochána in drugi (točka 42) in SpaceNet (točka 60).

[25] Glej sodbe La Quadrature du Net in drugi (točke od 120 do 122); Commissioner of An Garda Síochána in drugi (točka 48) in SpaceNet (točka 63).

[26] Glej sodbe La Quadrature du Net in drugi (točke od 120 do 122); Commissioner of An Garda Síochána in drugi (točka 49) in SpaceNet (točka 64).

[27] Glej sodbe La Quadrature du Net in drugi (točke od 127 do 129); Commissioner of An Garda Síochána in drugi (točki 50 in 51) in SpaceNet (točki 65 in 66).

[28] Glej sodbe La Quadrature du Net in drugi (točka 131); Commissioner of An Garda Síochána in drugi (točka 53) in SpaceNet (točka 68).

[29] Glej točko 41 in naslednje teh sklepnih predlogov.

bila opravljena komunikacija prek spleta. Če se hranijo samo IP-naslovi vira komunikacije, ne pa tudi njenega prejemnika, je tako stopnja občutljivosti te kategorije podatkov nižja od stopnje občutljivosti drugih podatkov o prometu. [30]

64. Sodišče hkrati poudarja, da – ker je IP-naslove mogoče uporabiti zlasti za izčrpno sledenje brskanju, ki ga je opravil uporabnik spleta, in torej njegovim spletnim dejavnostim – ti podatki omogočajo ugotavljanje njegovega podrobnega profila in natančno sklepanje o njegovem zasebnem življenju. Hramba in analiza teh IP-naslovov zato pomenita resna posega v temeljne pravice, določene s členoma 7 in 8 Listine, ter imata lahko odvračilni učinek na uresničevanje svobode izražanja, zagotovljene v členu 11 Listine. [31]

65. Vendar je treba v skladu z ustaljeno sodno prakso za potrebno uskladitev zadevnih pravic in zakonitih interesov, ki se zahteva s sodno prakso, upoštevati dejstvo, da je v primeru kaznivega dejanja, storjenega na spletu, IP-naslov lahko edino preiskovalno sredstvo, ki omogoča identifikacijo osebe, ki ji je bil v času storitve tega kaznivega dejanja ta naslov dodeljen. [32]

66. Sodišče zato meni, da zakonodajni ukrep, ki določa splošno in neselektivno hrambo zgolj IP-naslovov, dodeljenih viru povezave, načeloma ni v nasprotju s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter 52(1) Listine, pri čemer mora biti za to možnost določeno strogo spoštovanje materialnih in postopkovnih pogojev, ki morajo urejati uporabo teh podatkov, ter ob upoštevanju, da je glede na resnost posega, ki ga takšna hramba pomeni, mogoče navedeni poseg razen z zaščito nacionalne varnosti upravičiti zgolj z bojem proti hudemu kriminalu in preprečevanjem resnih groženj javni varnosti. [33]

67. Sodišče je poleg tega pojasnilo, da trajanje hrambe ne sme biti daljše od tega, kar je nujno potrebno z vidika zastavljenega cilja, in da je treba pri tovrstnem ukrepu določiti stroge pogoje in jamstva glede uporabe teh podatkov. [34]

3. Omejitve sodne prakse v zvezi z razlago člena 15(1) Direktive 2002/58/ES glede ukrepov za hrambo IP-naslovov, dodeljenih viru povezave

68. Kljub vsemu menim, da rešitev, do katere je prišlo Sodišče v zvezi z nacionalnimi ukrepi za hrambo IP-naslovov, dodeljenih viru povezave, če se razlagajo ob upoštevanju člena 15(1) Direktive 2002/58, vsebuje dve glavni težavi.

[30] Glej sodbo La Quadrature du Net in drugi (točka 152).

[31] Glej sodbe La Quadrature du Net in drugi (točka 153); Commissioner of An Garda Síochána in drugi (točka 73) in SpaceNet (točka 103) (Moj poudarek).

[32] Glej sodbe La Quadrature du Net in drugi (točka 154); Commissioner of An Garda Síochána in drugi (točka 73) in SpaceNet (točka 103).

[33] Glej sodbe La Quadrature du Net in drugi (točki 155 in 156); Commissioner of An Garda Síochána in drugi (točka 74) in SpaceNet (točki 104 in 105) (Moj poudarek).

[34] Glej sodbi La Quadrature du Net in drugi (točka 156) in SpaceNet (točka 105).

a) Uskladitev s sodno prakso v zvezi s sporočanjem IP-naslovov, dodeljenih viru povezave, v okviru tožb zaradi varstva pravic intelektualne lastnine

69. Na prvem mestu, kot sem že navedel v sklepnih predlogih v zadevi M.I.C.M.[35], ni nobenega dvoma o trenjih med to usmeritvijo sodne prakse in tisto v zvezi s sporočanjem IP-naslovov imetnikom pravic intelektualne lastnine v okviru tožb zaradi varstva teh pravic, v kateri je poudarjena obveznost držav članic, da imetnikom pravic intelektualne lastnine zagotovijo resnične možnosti plačila odškodnine za škodo, nastalo zaradi kršitve teh pravic[36].

70. Sodišče namreč v zvezi s to drugo usmeritvijo sodne prakse dosledno razsoja, da pravo Unije ne nasprotuje temu, da države članice določijo obveznost, da se osebam zasebnega prava posredujejo osebni podatki, zato da lahko pred civilnimi sodišči začnejo postopke zaradi kršitev avtorskih pravic.[37]

71. Sodišče v zvezi s tem ugotavlja, da možnost držav članic, da določijo obveznost razkritja osebnih podatkov v okviru civilnega sodnega postopka, izhaja najprej iz možnosti določitve takega razkritja v okviru pregona kaznivih dejanj[38], ki je bil nato razširjen na področje civilnega prava.

72. Vendar Sodišče, kar zadeva IP-naslove, hkrati nalaga, da je mogoče te podatke hraniti le v okviru boja proti hudemu kriminalu in preprečevanja resnih groženj javni varnosti.[39]

73. Menim, da poskusi uskladitve teh dveh usmeritev sodne prakse privedejo do neprilagojenih rezultatov, ki ne prepričajo.

74. Na eni strani v nasprotju s tem, kar je trdila francoska vlada na obravnavi, boja proti kršitvam pravic intelektualne lastnine ni mogoče uvrstiti v okvir boja proti hudemu kriminalu. Menim, da je treba pojem „hud kriminal“ razlagati samostojno. Ne more biti odvisen od njegovega pojmovanja v posameznih državah članicah, saj bi v tem primeru omogočili izogibanje zahtevam člena 15(1) Direktive 2002/58 glede na to, ali države članice boj proti hudemu kriminalu pojmujejo široko ali ozko. Kot sem že navedel, interesov, povezanih z varstvom pravic intelektualne lastnine, ni mogoče mešati z interesi, na katerih temelji boj proti hudemu kriminalu.[40]

75. Na drugi strani bi bila dopustitev posredovanja IP-naslovov imetnikom pravic intelektualne lastnine v okviru postopkov, katerih predmet je varstvo teh pravic, čeprav je njihova hramba omogočena zgolj v okviru boja proti hudemu kriminalu, očitno v nasprotju s sodno prakso Sodišča v zvezi s hrambo podatkov o povezavi, s čimer bi bil pogojem, ki se zahtevajo za hrambo takih podatkov, odvzet polni učinek, saj bi se do njih vsekakor lahko dostopalo iz drugačnih razlogov.

76. Iz tega po mojem mnenju izhaja, da bi bila hramba IP-naslovov zaradi varstva pravic intelektualne lastnine in za njihovo sporočanje imetnikom teh pravic v okviru postopkov, katerih predmet je to varstvo, lahko v nasprotju s členom 15(1) Direktive 2002/58, kot se razlaga v sodni praksi Sodišča. Obveznost, da se osebam zasebnega prava posredujejo osebni podatki, zato da

35 C-597/19, EU:C:2020:1063, točka 98.

36 Glej moje sklepne predloge v zadevi M.I.C.M. (C-597/19, EU:C:2020:1063, točka 97).

37 Glej sodbe z dne 19. aprila 2012, Bonnier Audio in drugi (C-461/10, EU:C:2012:219, točka 55); z dne 4. maja 2017, Rīgas satiksme (C-13/16, EU:C:2017:336, točka 34), in z dne 17. junija 2021, M.I.C.M. (C-597/19, EU:C:2021:492, točke od 47 do 54).

38 Glej v tem smislu sodbo z dne 29. januarja 2008, Promusicae (C-275/06, EU:C:2008:54, točke od 50 do 52).

39 Glej točko 65 teh sklepnih predlogov.

40 Glej moje sklepne predloge v zadevi M.I.C.M. (C-597/19, EU:C:2020:1063, točka 103).

lahko pred civilnimi sodišči začnejo postopke zaradi kršitev avtorskih pravic, ki jo je sicer omogočilo tudi samo Sodišče, je torej istočasno izničena zaradi učinkov njegove lastne sodne prakse v zvezi s hrambo IP-naslovov s strani ponudnikov elektronskih komunikacijskih storitev.

77. Vendar taka rešitev ni zadovoljiva, saj bi bilo s tem omajano ravnotežje med različnimi zadevnimi interesi, ki ga je želelo vzpostaviti Sodišče, ker bi imetniki pravic intelektualne lastnine tako ostali brez glavnega, če ne edinega sredstva za identifikacijo storilcev kršitev navedenih pravic na spletu. Ta preudarek me je privedel do druge težave, ki lahko po mojem mnenju izhaja iz sodne prakse Sodišča, kar zadeva nacionalne ukrepe, katerih namen je hramba IP-naslovov, dodeljenih viru povezave, če se razlaga ob upoštevanju člena 15(1) Direktive 2002/58.

b) Tveganje sistemske nekaznovanosti kršitev, storjenih izključno na spletu

78. Tako, na drugem mestu, menim, da je taka rešitev vir praktičnih težav. Kot je poudarilo Sodišče, je v primeru kršitve, storjene izključno na spletu, IP-naslov lahko edino preiskovalno sredstvo, ki omogoča identifikacijo osebe, ki ji je bil ta naslov dodeljen ob storitvi te kršitve.

79. Vendar se mi zdi, da se ta element pri tehtanju zadevnih interesov ne upošteva v celoti. Ker Sodišče možnost hrambe IP-naslovov kljub vsemu omejuje na okvir boja proti hudemu kriminalu, hkrati izključuje možnost, da bi se ti podatki lahko hranili zaradi boja proti kaznivim dejanjem na splošno, čeprav je mogoče nekatere od teh kršitev preprečiti, odkriti ali sankcionirati samo po zaslugi navedenih podatkov.

80. Z drugimi besedami, sodna praksa Sodišča bi lahko privedla do tega, da bi nacionalni organi ostali brez edinega sredstva za identifikacijo storilcev kršitev, ki so bile storjene na spletu, vendar ne spadajo v okvir hudega kriminala, kot so kršitve pravic intelektualne lastnine. To bi dejansko privedlo do sistemske nekaznovanosti kršitev, storjenih izključno na spletu, in sicer ne zgolj kršitev pravic intelektualne lastnine. Na misel mi pridejo zlasti dejanja obrekovanja, storjena na spletu. Pravo Unije sicer določa odreditev ukrepov zoper posrednike, katerih storitve so uporabljene za storitev takih kršitev,[41] vendar bi lahko sodna praksa Sodišča privedla do tega, da ne bi bilo mogoče nikoli uvesti kazenskega postopka zoper same storilce teh kršitev.

81. Razen če naj se dopusti, da ni mogoče cele vrste kaznivih dejanj nikoli preganjati, menim, da bi bilo treba na novo analizirati ravnotežje med različnimi zadevnimi interesi.

82. Na podlagi teh različnih preudarkov želim Sodišču predlagati, naj nekoliko prilagodi sodno prakso v zvezi z nacionalnimi ukrepi za hrambo IP-naslovov, kot se razlagajo ob upoštevanju člena 15(1) Direktive 2002/58.

4. Predlog za prilagoditev sodne prakse Sodišča v zvezi z razlago člena 15(1) Direktive 2002/58/ES glede ukrepov za hrambo IP-naslovov, dodeljenih viru povezave

83. Ob upoštevanju zgornjih preudarkov menim, da bi bilo treba člen 15(1) Direktive 2002/58 razlagati tako, da ne nasprotuje ukrepom, ki določajo splošno in neselektivno hrambo IP-naslovov, dodeljenih viru povezave, za obdobje, ki je časovno omejeno na to, kar je nujno

[41] Glej člen 15(1) Direktive 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 25, str. 399).

potrebno, zato da se tako zagotovijo preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj na spletu, za katera je IP-naslov *edino* preiskovalno *sredstvo*, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve kršitve dodeljen.

84. V zvezi s tem moram poudariti, da – glede na resnost posega v temeljne pravice, določene s členoma 7 in 8 Listine, ki ga hramba podatkov pomeni – ta predlog po mojem mnenju ne omaje zahteve po sorazmernosti, katere izpolnitev se zahteva za to hrambo.[42] Nasprotno, v celoti jo izpolnjuje.

85. Po eni strani se z omejitvijo pravic in obveznosti, določenih s členi 5, 6 in 9 Direktive 2002/58, ki jo pomeni hramba IP-naslovov, uresničuje cilj splošnega interesa, katerega pomembnost je v sorazmerju s to težo, in sicer cilj preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj, določenih z zakoni, ki sicer ne bi imeli nobenega učinka.

86. Po drugi strani se ta omejitev izvaja v mejah tega, kar je nujno potrebno. Taka hramba je namreč omejena na natančne predpostavke, to je kazniva dejanja, storjena na spletu, katerih storilca je mogoče identificirati samo z IP-naslovom, ki mu je bil dodeljen. Povedano drugače, ne gre za to, da bi dovolili splošno in neselektivno hrambo podatkov brez drugih pogojev, ampak samo za to, da se omogoči pregon kaznivih dejanj ne na splošno, ampak zgolj točno določenih.

87. Vendar, čeprav člen 15(1) Direktive 2002/58 ne nasprotuje splošni in neselektivni hrambi IP-naslovov, dodeljenih viru povezave, da se tako zagotovijo preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj na spletu, za katera je IP-naslov edino preiskovalno sredstvo, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve kršitve dodeljen, je treba kljub vsemu še dodati, da je treba v skladu s sodno prakso za to možnost določiti „strogo spoštovanje materialnih in postopkovnih pogojev, *ki morajo urejati uporabo teh podatkov*“.[43] Sodišče je poleg tega pojasnilo, da je treba pri tovrstnem ukrepu „določiti stroge pogoje in jamstva glede *uporabe teh podatkov*“.[44]

88. Povedano drugače in kot sem že poudaril, hrambe podatkov in dostopa do njih ni mogoče obravnavati ločeno. V teh okoliščinah sicer možnost, ki jo ima Hadopi, da dostopa do IP-naslovov, ni že v izhodišču v nasprotju s členom 15(1) Direktive 2002/58, če so se ti podatki hranili v skladu z zahtevami iz te določbe, vendar je treba za odgovor na vprašanja za predhodno odločanje, ki so bila predložena Sodišču, še preučiti, ali so pogoji dostopa do IP-naslovov, dodeljenih viru povezave, ki ga ima Hadopi, sami po sebi v skladu z navedeno določbo, predvsem v zvezi s tem, ali je ali ni potrebno, da sodišče ali neodvisen upravni organ opravi predhodni nadzor nad takim dostopom.

89. Po analizi uvodnega vprašanja hrambe IP-naslovov, dodeljenih viru povezave, bom preučil še dostop do teh podatkov s strani Hadopi ob upoštevanju člena 15(1)Direktive 2002/58.

[42] Glej točki 60 in 61 teh sklepnih predlogov.

[43] Glej sodbo La Quadrature du Net in drugi (točka 155) (Moj poudarek).

[44] Glej sodbo La Quadrature du Net in drugi (točka 156) (Moj poudarek).

5. Dostop do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, s strani Hadopi

90. Iz sodne prakse Sodišča v zvezi s cilji, ki bi lahko utemeljevali nacionalni ukrep, ki odstopa od načela zaupnosti elektronskih komunikacij, je razvidno, da mora dostop do podatkov strogo in objektivno ustrezati enemu od teh ciljev ter da mora biti cilj, ki se želi doseči s tem ukrepom, sorazmeren s težo posega v temeljne pravice, ki ga povzroči navedeni dostop.[45]

91. Poleg tega je, kot sem že pojasnil[46], dostop do podatkov, ki jih hranijo ponudniki v skladu z ukrepom, sprejetim na podlagi člena 15(1) Direktive 2002/58, načeloma mogoče upravičiti zgolj s ciljem v splošnem interesu, za katerega je bila navedena hramba tem ponudnikom naložena[47].

92. Sodišče je tako razsodilo, da lahko v skladu z načelom sorazmernosti na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj resen poseg upraviči le cilj boja proti kriminalu, ki mora biti prav tako opredeljen kot „resen“.[48]

93. V zvezi s tem v nasprotju s trditvami francoske vlade in Komisije ugotavljam, da dostop Hadopi do podatkov o civilni identiteti, ki ustrezajo IP-naslovu, pomeni resen poseg v temeljne pravice. Ne gre namreč samo za dostopanje do podatkov o civilni identiteti, ki so sami zase podatki nizke občutljivosti, ampak za povezovanje teh podatkov z veliko širšim sklopom podatkov, to je IP-naslovom, in tudi, kot poudarjajo tožeče stranke iz postopka v glavni stvari, izvlečkom datoteke, s prenosom katere je bila kršena avtorska pravica. Gre torej za povezovanje civilne identitete osebe z vsebino ogledane datoteke in IP-naslovom, prek katerega je bil ta ogled izveden.

94. Vendar bi bilo po mojem mnenju treba – enako kot menim, da je treba dovoliti tudi hrambo podatkov, ki pomeni resen poseg v temeljne pravice, zato da se tako zagotovijo preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj na spletu, za katera je IP-naslov edino preiskovalno sredstvo, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve kršitve dodeljen[49] – zaradi uresničevanja istega cilja omogočiti tudi dostop do teh podatkov, sicer bi dopustili splošno nekaznovanost kršitev, storjenih izključno na spletu.

95. Dostop, ki ga ima Hadopi do podatkov o civilni identiteti, povezanih z IP-naslovom, se mi torej zdi utemeljen s ciljem v splošnem interesu, za katerega je bila ponudnikom elektronskih komunikacijskih storitev ta hramba naložena.

96. Vendar je v sodni praksi Sodišča pojasnjeno, da nacionalna zakonodaja, ki ureja dostop pristojnih organov do shranjenih podatkov o prometu in podatkov o lokaciji, ne more zgolj zahtevati, da je dostop v skladu s ciljem te zakonodaje, temveč mora določiti tudi materialne in postopkovne pogoje, ki urejajo dostop pristojnih nacionalnih organov do zadevnih podatkov.[50]

97. Natančneje, Sodišče je razsodilo, da – ker ni mogoče šteti, da je splošni dostop do vseh shranjenih podatkov, neodvisno od kakršne koli povezave, tudi posredne, s ciljem, ki se želi doseči, omejen na to, kar je nujno potrebno – se mora nacionalna ureditev pri določitvi okoliščin in pogojev, pod katerimi se pristojnim nacionalnim organom omogoči dostop do podatkov

45 Glej sodbi z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točka 55), in Prokuratuur (točka 32).

46 Točka 47 teh sklepnih predlogov.

47 Glej sodbe SpaceNet (točka 131); La Quadrature du Net in drugi (točka 166) in Commissioner of An Garda Síochána in drugi (točka 98).

48 Glej sodbe Tele2 (točka 115); z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točka 56), in Prokuratuur (točka 33).

49 Glej točko 65 in naslednje teh sklepnih predlogov.

50 Glej sodbe Tele2 (točka 118); Prokuratuur (točka 49) in Commissioner of An Garda Síochána in drugi (točka 104).

uporabnikov, opreti na objektivna merila, zato da se zagotovi, da je dostop odobren le do podatkov oseb, za katere obstaja sum, da nameravajo izvršiti ali da so izvršile hudo kaznivo dejanje ali da so bile tako ali drugače pri takem kaznivem dejanju udeležene.[51]

98. Tako je v skladu s sodno prakso za zagotovitev popolnega spoštovanja teh pogojev v praksi bistveno, da je dostop pristojnih nacionalnih organov do shranjenih podatkov načeloma pogojen s predhodnim nadzorom, ki ga opravi sodišče ali neodvisen upravni organ.[52]

99. Vendar ugotavljam, da je Sodišče to potrebo po predhodnem nadzoru nad dostopom do osebnih podatkov izoblikovalo v posebnih okoliščinah, ki se razlikujejo od obravnavane zadeve in so zajemale *posebej resna* vmešavanja v zasebno življenje uporabnikov elektronskih komunikacijskih storitev.

100. V vsaki od sodb, v katerih je bila poudarjena ta zahteva, je šlo namreč za nacionalne ukrepe, s katerimi je bil dovoljen dostop do vseh podatkov o prometu in lokaciji uporabnikov v zvezi z vsemi sredstvi elektronske komunikacije[53] ali vsaj v zvezi s fiksno in mobilno telefonijo[54]. Natančneje, šlo je za dostop do „vseh podatkov […], iz katerih bi bile lahko razvidne informacije o komunikacijah, ki jih je uporabnik opravil z uporabo elektronskih komunikacijskih sredstev, ali o lokaciji uporabljene terminalske opreme, in iz katerih bi bilo mogoče natančno sklepati o njegovem zasebnem življenju“,[55] tako da zahteva po predhodnem nadzoru, ki ga opravi sodišče ali neodvisen upravni organ, za dostop do teh podatkov po mojem mnenju obstaja le v teh okoliščinah.

101. Vendar ostaja na eni strani dostop, ki ga ima Hadopi, omejen na to, da se podatki o civilni identiteti povežejo z uporabljenim IP-naslovom in datoteko, ogledano v točno določenem trenutku, ne da bi bila zato pristojnim organom omogočena rekonstrukcija spletnih poizvedb zadevnega uporabnika, kar pomeni, da ne morejo izpeljati niti natančnih ugotovitev o njegovem zasebnem življenju, ki bi presegale seznanitev z natančno določeno datoteko, ogledano v času storitve kršitve. Torej se ne omogoči sledenje vsem spletnim dejavnostim zadevnega uporabnika.

102. Na drugi strani se ti podatki nanašajo samo na podatke oseb, ki so – kot je bilo ugotovljeno v zapisnikih, ki so jih pripravile organizacije imetnikov pravic – storile dejanja, ki bi lahko pomenila kršitev obveznosti, določene s členom L.336 3 CPI. Dostop, ki ga ima Hadopi do podatkov o civilni identiteti, povezanih z IP-naslovi, je torej strogo omejen na to, kar je potrebno za uresničitev zastavljenega cilja, to je omogočiti preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj na spletu, za katera je IP-naslov edino preiskovalno sredstvo, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve kršitve dodeljen, pri čemer to sredstvo zajema mehanizem postopnega odgovora.

103. V teh okoliščinah menim, da člen 15(1) Direktive 2002/58 ne nalaga, da mora sodišče ali neodvisen upravni organ opraviti predhodni nadzor nad dostopom, ki ga ima Hadopi do podatkov o civilni identiteti, povezanih z IP-naslovi uporabnikov.

[51] Glej sodbe Tele2 (točka 119); Prokuratuur (točka 50) in Commissioner of An Garda Síochána in drugi (točka 105).

[52] Glej sodbe Tele2 (točka 120); Prokuratuur (točka 50) in Commissioner of An Garda Síochána in drugi (točka 106).

[53] Glej sodbi Tele2 ter Commissioner of An Garda Síochána in drugi.

[54] Glej sodbo Prokuratuur.

[55] Glej sodbo Prokuratuur (točka 45).

104. V preostalem ugotavljam še – kot poudarja francoska vlada – da dostopa, ki ga ima do teh podatkov Hadopi, sicer res predhodno ne nadzira sodišče ali neodvisen organ, vendar to še ne pomeni, da se nad njim ne izvaja nikakršen nadzor, saj datoteko, ki jo Hadopi pošlje operaterjem elektronskih komunikacij, vsak dan sestavi zapriseženi uslužbenec na podlagi prejetih zadev, ki se pred priložitvijo datoteki potrdijo na podlagi naključnih vzorcev.[56] Predvsem pa je treba ugotoviti, da se za postopek postopnega odgovora po mojem mnenju še naprej uporabljajo določbe Direktive (EU) 2016/680.[57] Na tej podlagi so fizične osebe, ki jih obravnava Hadopi, upravičene do vseh materialnih in postopkovnih jamstev, določenih s to direktivo. Ta zajemajo pravico dostopa do osebnih podatkov, ki jih obdeluje Hadopi, njihovega popravka in izbrisa ter možnost vložitve pritožbe pri neodvisnem nadzornem organu, ki ji lahko po potrebi sledi vložitev pravnega sredstva pod pogoji, določenimi s splošnim pravom.[58]

105. Torej predlagam, naj se na prvo in drugo vprašanje za predhodno odločanje odgovori, da je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da ne nasprotuje nacionalni ureditvi, ki ponudnikom storitev elektronskih komunikacij omogoča hrambo, upravnemu organu, pristojnemu za varstvo avtorske in sorodnih pravic pred kršitvami teh pravic, storjenimi na spletu, pa dostop samo do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, zato da lahko ta organ identificira imetnike teh naslovov, v zvezi s katerimi je podan sum, da so odgovorni za te kršitve, in lahko po potrebi v zvezi z njimi sprejme ukrepe brez predhodnega nadzora sodišča ali neodvisnega upravnega organa nad tem dostopom, če so ti podatki edino preiskovalno sredstvo, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve kršitve dodeljen.

B. Tretje vprašanje za predhodno odločanje

106. Predložitveno sodišče želi s tretjim vprašanjem za predhodno odločanje izvedeti, ali je treba v primeru pritrdilnega odgovora na prvo in drugo vprašanje ter ob upoštevanju nizke občutljivosti podatkov o civilni identiteti, strogih pravil, ki veljajo za dostop do podatkov, in nujnosti, da se ne ogrozi naloga javne službe, zaupana zadevnemu upravnemu organu, člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da nasprotuje temu, da se predhodni nadzor nad dostopom opravlja na prilagojen način, na primer v obliki avtomatiziranega nadzora, po potrebi s pregledom interne službe organa, katerega neodvisnost in nepristranskost v razmerju do uradnikov, ki so zadolženi za navedeno zbiranje podatkov, je zajamčena.

107. Iz besedila tretjega vprašanja za predhodno odločanje in pisnega odgovora francoske vlade na vprašanja Sodišča je razvidno, da se prilagojeni način nadzora, na katerega je napoteno v tem vprašanju, ne nanaša na nadzorni mehanizem, ki v nacionalnem pravu že obstaja, ampak na možnosti, ki bi se lahko preučile in s katerimi bi bilo mogoče francoski mehanizem po potrebi uskladiti s pravom Unije.

[56] Dodatno še ugotavljam, da je mogoče nasprotovanje sistematični obveznosti predhodnega nadzora utemeljiti tudi z razlogi, ki se nanašajo na izvedljivost. Za obstoj organiziranega sistema boja proti kršitvam avtorske pravice, storjenim na spletu, kakršen je ta iz postopka v glavni stvari, je treba obdelati velike količine osebnih podatkov, ki ustrezajo številu preganjanih kršitev, kar po navedbah francoske vlade na primer za leto 2019 pomeni 33.465 zahtev za identifikacijo IP-naslova, ki jih je vsak dan izvedla Hadopi. V tem okviru bi obveznost predhodnega nadzora nad dostopom do teh podatkov lahko v praksi ogrozila delovanje mehanizmov organiziranega boja proti kršitvam teh pravic na spletu, s čimer bi bilo omajano ravnotežje med pravicami uporabnikov in pravicami avtorjev.

[57] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL 2016, L 119, str. 89).

[58] Vsa ta jamstva so določena z določbami poglavja III, naslov III, zakona št. 78-17 o informatiki, datotekah in svoboščinah z dne 6. januarja 1978 (JORF z dne 7. januarja 1978).

108. V skladu z ustaljeno sodno prakso pa namen predloga za sprejetje predhodne odločbe ni oblikovanje posvetovalnih mnenj o splošnih in hipotetičnih vprašanjih, ampak dejanska potreba po učinkoviti rešitvi spora, ki se nanaša na pravo Unije. [59]

109. Tretje vprašanje za predhodno odločanje je torej po mojem mnenju hipotetično, zato ga je treba razglasiti za nedopustno.

110. Ob upoštevanju odgovora, ki ga predlagam na prvo in drugo vprašanje za predhodno odločanje, na tretje vprašanje nikakor ni treba odgovoriti.

V. Predlog

111. Ob upoštevanju vseh navedenih ugotovitev Sodišču predlagam, naj na vprašanja za predhodno odločanje, ki jih je predložil Conseil d'État (državni svet, Francija), odgovori:

Člen 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) v povezavi s členi 7, 8, 11 in 52(1) Listine Evropske unije o temeljnih pravicah

je treba razlagati tako, da

ne nasprotuje nacionalni ureditvi, ki ponudnikom storitev elektronskih komunikacij omogoča hrambo, upravnemu organu, pristojnemu za varstvo avtorskih in sorodnih pravic pred kršitvami teh pravic, storjenimi na spletu, pa dostop samo do podatkov o civilni identiteti, ki ustrezajo IP-naslovom, zato da lahko ta organ identificira imetnike teh naslovov, v zvezi s katerimi je podan sum, da so odgovorni za te kršitve, in lahko po potrebi v zvezi z njimi sprejme ukrepe brez predhodnega nadzora sodišča ali neodvisnega upravnega organa nad tem dostopom, če so ti podatki edino preiskovalno sredstvo, s katerim je mogoče identificirati osebo, ki ji je bil ta naslov v času storitve kršitve dodeljen.

[59] Glej sodbe z dne 26. oktobra 2017, Balgarska energiyna borsa (C-347/16, EU:C:2017:816, točka 31); z dne 31. maja 2018, Confetra in drugi (C-259/16 in C-260/16, EU:C:2018:370, točka 63), in z dne 17. oktobra 2019, Elektrorazdelenie Yug (C-31/18, EU:C:2019:868, točka 32).